



RATGEBER

Hybride UEM-Strategie mit ACMP Intune Management

Wie Sie durch die Kombination von ACMP und Intune mehr Flexibilität, Sicherheit und Kontrolle bei der Verwaltung von Endgeräten realisieren können.

Der Weg zur hybriden UEM-Strategie

Die zunehmende Verlagerung von IT-Infrastrukturen in die Cloud stellt Unternehmen vor die Herausforderung, bestehende On-Premises-Systeme mit cloud-basierten Lösungen zu kombinieren. Die Aagon Client Management Platform (ACMP) bietet durch die Kombination mit Microsoft Intune dafür die ideale Lösung: ein hybrides Unified Endpoint Management (UEM) für 100 Prozent Transparenz, Kontrolle und Sicherheit bei der Geräteverwaltung.

Effektive Verwaltung aller Endgeräte auf einer einheitlichen Plattform

ACMP gibt IT-Administratoren die Möglichkeit, bestehende Microsoft-Intune-Instanzen in ACMP zu integrieren, um eine einheitliche Plattform für effektives Hybrid-UEM (Unified Endpoint Management) zu schaffen.



**VORTEILE VON CLOUD UND
ON-PREMISES NUTZEN**



**MEHR EFFIZIENZ
UND SICHERHEIT**



**ZENTRALE VERWALTUNG
ÜBER DIE ACMP SUITE**

Cloud-UEM und mobile Endgeräte

Die Verwaltung von Endgeräten in Unternehmen hat sich in den letzten Jahren stark weiterentwickelt. Das Spektrum der Clients reicht heute weit über klassische Desktops hinaus. Mobile Betriebssysteme wie iOS und Android müssen einbezogen werden, und eine verteilte Infrastruktur aus Homeoffice und Inhouse-Arbeitsplätzen entzieht die Gesamtheit der Endgeräte dem direkten physischen Zugriff. Hinzu kommen wachsende Sicherheitsbedrohungen. Ransomware-Angriffe nehmen jährlich zu – inzwischen gibt es ein regelrechtes Ransomware-as-a-Services-Geschäftsfeld.

Mit gleichbleibender Personalstärke müssen Administrationsabteilungen Systeme aktuell halten und auf Schwachstellen reagieren. Sie müssen den Datenschutz im Auge behalten, ISO-Normen und gesetzliche Regularien wie etwa NIS-2 und DORA erfüllen und dafür zusätzliche Dokumentationen erstellen und Vorkehrungen treffen.

32 Prozent der Remote- und Hybrid-Worker nutzen nicht von der IT-Abteilung genehmigte Apps oder Software für ihre Arbeit.

Quelle: Studie „The State of Remote Work Security“ von Lookout, 2023

Der traditionelle Ansatz bestand darin, mit lokal betriebenen Client-Management-Systemen PCs, Server und mobile Devices mit Windows- oder Linux-Betriebssystemen zentral und automatisiert zu verwalten. Er führte weiter hin zu cloud-basierten UEM-Systemen. Das bekannteste – und gebräuchlichste – von ihnen ist Microsoft Intune, da es bereits in den Microsoft 365 Enterprise-Lizenzpaketen enthalten ist.

Größter Vorteil dieser Lösungen ist ihre einfache Skalierbarkeit, die ständige Aktualisierung und der Wegfall eigener Infrastrukturkosten. Administrationsaufwände werden minimiert, da sich Wartung und Updates automatisiert über den Cloud-Anbieter regeln.

Gleichzeitig steigt damit die Abhängigkeit von der Verfügbarkeit der Cloud-Plattform und einer stabilen Internetverbindung. Die nativen Verwaltungsfunktionen eines Client-Betriebssystems sind häufig nur eingeschränkt nutzbar oder nicht mit anderen Systemen vernetzt. Ein Cloud-UEM setzt meist auf die mobile Schnittstelle des Geräts, die im Vergleich zu einem lokalen Agenten deutlich weniger Steuerungsmöglichkeiten bietet. Weist man einem Gerät oder einer Gruppe von Geräten ein Software-Update zu, bleibt nur abzuwarten, wann etwas passiert. Der Zeitpunkt des Updates lässt sich nicht beeinflussen, da der Cloud-Anbieter eigenständig entscheidet, wann Sicherheitslücken geschlossen oder Updates ausgerollt werden.

Einschränkungen von Microsoft Intune

Am Beispiel Intune zeigen sich exemplarisch die Stärken und Schwächen einer cloud-basierten Lösung. Das Microsoft-Tool bietet mit Funktionen wie der Verteilung von Exe- und MSI-Dateien oder der Remotesperre eine solide Grundlage für das Management mobiler Endgeräte. Doch die Grenzen werden schnell sichtbar: Server lassen sich nur mit Zusatz-Tools verwalten, SNMP-Geräte bleiben außen vor, es sei denn, Unternehmen investieren in kostenpflichtige Erweiterungen. Dadurch erhalten Admins oft nur einen unvollständigen Überblick über ihre IT-Infrastruktur, was sowohl Sicherheitsrisiken als auch Ineffizienzen begünstigt.

Zur Ergänzung von Intune empfiehlt Microsoft den Einsatz von Co-Management:

„Co-management enables you to concurrently manage Windows 10 or later devices by using [...] [an Endpoint Manager] and Microsoft Intune. It lets you cloud-attach your existing investment [...] by adding new functionality. By using co-management, you have the flexibility to use the technology solution that works best for your organization.“

Quelle: <https://learn.microsoft.com/en-us/intune/configmgr/comanage/overview>, (Stand: 12.04.2024)



On-Premises: Hohe Funktionalität und Datenschutz

On-Premises-UEM-Systeme demgegenüber werden auf eigenen Servern betrieben – sei es lokal oder in einer Private Cloud – und verfügen über spezialisierte Agenten, die eine umfassende Kontrolle ermöglichen. Microsoft-Dienste (WSUS-Alternative, Defender, BitLocker) lassen sich nahtlos integrieren, ohne auf eine Cloud-Anbindung angewiesen zu sein.

Ein entscheidender Vorteil ist die Datenhoheit (beim Betrieb eigener Server): Sensible Informationen verbleiben innerhalb der eigenen Infrastruktur und werden nicht für KI-Trainingszwecke verwendet, was in der Cloud immer geschehen kann. Gleichzeitig ist beim lokalen Betrieb der rechtliche Aufwand geringer. Datenverarbeitungsverträge mit Dienstleistern müssen nicht aufwändig verhandelt werden beziehungsweise beschränken sich auf die eigentliche Geschäftsbeziehung und eben nicht auf Firmen- oder Kundendaten.

Eine lokale UEM-Lösung macht das Unternehmen des Weiteren unabhängig von Internet- oder Serverstörungen des Cloud-Anbieters; die eigene Infrastruktur bleibt steuerbar. Sie ist auch im Hinblick auf Compliance oft die bessere Wahl. Strenge Vorgaben in sicherheitskritischen Bereichen, die Unabhängigkeit vom Internet vorschreiben – etwa im Umfeld von KRITIS und NIS-2 – lassen sich mit On-Premises-Systemen besser umsetzen. Sie sind bei Unternehmen, die in diesem Bereich etwas tun müssen, daher die bevorzugte Betriebsform.

Zudem können mit einer (mandantenfähigen) UEM-Lösung im eigenen Haus Sicherheitszonen individueller konfiguriert werden als bei einem Cloud-System „von der Stange“. Komplexe Infrastrukturen (Standorte, Arbeitsbereiche) sind über die Lösung verwaltbar, in einem Mix aus online (Verwaltungsabteilungen inkl. Homeoffice) und offline (Produktion, eigene Abteilung & Netz). Mit Low-Code/No-Code werden vorgefertigte Bausteine zur Desktop Automation flexibel variiert, bis hin zu Formularen (die auch ohne Internet verfügbar sind).

Auf der anderen Seite sind On-Premises-Lösungen mit Investitionen in Hardware und Lizenzen verbunden. Skalierungsprozesse erfordern Zeit und finanzielle Ressourcen. Und die nur eingeschränkte Unterstützung mobiler Endgeräte erweist sich in einer zunehmend mobilen Arbeitswelt inzwischen als Nachteil.

Hybrides Endgerätemanagement als Königsweg

Der vielversprechendste Ansatz liegt daher in einer hybriden Strategie, wie sie Aagon durch die Integration von Microsoft Intune in die ACMP Suite geschaffen hat. Geräte-, Benutzer-, Gruppen- und App-Daten aus Intune werden dabei in die UEM-Lösung überführt, sind darin sichtbar und lassen sich detailliert managen – in ACMP, über Intune.

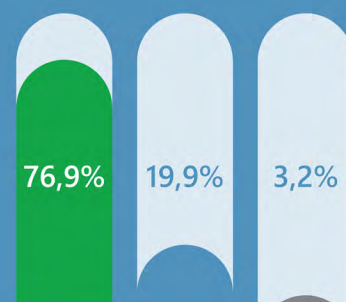
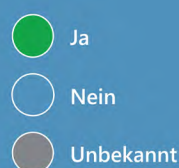
Die Kombination aus Cloud-UEM und On-Premises-Management vereint die Stärken beider Welten. Unter dem Motto „Better together!“ entsteht eine klar strukturierte Client-Landschaft, die über die ACMP Console zentral und benutzerfreundlich verwaltet werden kann – für höhere Effizienz, bessere Transparenz und maximale Sicherheit.

Unternehmen können dadurch sowohl lokale als auch mobile Endgeräte effizient verwalten und sind zugleich weniger anfällig für Ausfälle. Ein Teil der Geräte ist meist immer erreichbar und verwaltbar, egal ob der eigene Server ausfällt oder die Cloud.

Über 75% sehen in der Kombination aus On-Premise und Cloud einen zukunftsorientierten Ansatz.

Quelle: Research in Action

Frage: „Empfinden Sie den Ansatz einer hybriden Infrastruktur aus einer On-Premise UEM-Lösung und der Integration von Microsoft Intune als eine zukunftsorientierte Lösung?“



1000 Befragte in der DACH Region
© 2025, Research In Action GmbH

EINHEITLICHE PLATTFORM

Verwaltung der gesamten Infrastruktur: Von mobilen Endgeräten über PCs bis hin zu Servern.

ZENTRALE VERWALTUNG

Prozesse zentral in einer Konsole automatisieren: Von Update- und Patch-Management bis zu MS Defender.

HYBRIDES UEM

Alle Komponenten erreichen: Egal ob in der Cloud oder On-Premises.

Updates besser nachverfolgen

Die Administrationsabteilung hat einen klaren Überblick darüber, welche Geräte entweder ausschließlich durch Intune oder durch das On-Premises-UEM verwaltet werden. ACMP Agenten lassen sich problemlos auf Intune-Geräten installieren. Dies führt zu einer verbesserten Nachverfolgbarkeit. Zwar können auch in Intune Apps Gruppen zugewiesen werden, jedoch fehlt die Transparenz darüber, wann die Installation tatsächlich erfolgt.

Dasselbe gilt für Patches. Mit ACMP Intune Management lassen sich solche Prozesse präzise überwachen und umfassend reporten.

Flexibilität & Skalierbarkeit

Administrationsabteilungen können mit ACMP Intune Management ihre UEM-Infrastruktur flexibel und skalierbar gestalten. Durch die Integration lokaler Systeme und cloud-basierter Ressourcen verwalten sie diverse Endpunkte (Windows, MacOS, Android, iOS, Linux) für nahtlose Abläufe, egal wo sich die Geräte befinden. Skalierbarkeit bedeutet: Start mit einer Cloud-Infrastruktur und anschließend schrittweiser Ausbau des Systems on-premises, um zusätzliche Kapazitäten und Funktionen zu nutzen.

SOAR-Konzept

Seit einiger Zeit sind in ACMP neben den Modulen für Patch Management, Desktop Automation, Inventarisierung, Lizenzmanagement, Asset Management und OS Deployment auch weitere Microsoft-eigene Security-Tools wie Defender- und BitLocker-Management verfügbar. Auf ihnen bauen Schwachstellenmanagement, Third-Party-Patch-Management und Windows-Update-Management auf. Besonders letzteres zeigt sich als Vorteil, da Intune diese Funktion standardmäßig nur für Clients bietet, während es für Server mit zusätzlichem Aufwand verbunden ist.

Mit dem SOAR (Security Orchestration, Automation and Response)-Konzept bietet ACMP hier also eine umfassende Sicherheitslösung. Dadurch lassen sich Sicherheitsbedrohungen automatisch erkennen und neutralisieren. Während Intune vorwiegend auf mobile Geräte ausgerichtet ist, deckt ACMP die restliche IT-Infrastruktur ab. So entsteht eine hybride Umgebung, in der Sicherheitsrisiken schnell und effizient abgewehrt werden können.

Funktionen und Vorteile von ACMP Intune Management

Umfassendes Reporting

Klares, umfassendes Reporting über die gesamte IT, ohne den Wechsel zwischen Tools.

App-Verteilung

Über Intune können Administratoren Apps zentral bereitstellen.

Mobile Device Management

Intune überzeugt besonders in der Verwaltung mobiler Endgeräte (Mobile Device Management, MDM).

Patch Management für Drittanbieter

Automatisierte und getestete Updates in ACMP zuverlässig bereitstellen.

Asset Management

Vollständige Übersicht über sämtliche IT-Assets des Unternehmens.

OS Deployment

ACMP ermöglicht einen Bare-Metal-Rollout, also die Bereitstellung von Betriebssysteme auf Hardwareebene.

Windows Update Management

Umfassende Lösung für Windows Client- und Server-Updates, inklusive Testprozesse und Microsoft 365-Integration, ganz ohne WSUS oder weitere Microsoft-Cloud-Dienste.

Fazit:

Die perfekte Symbiose für ein modernes, hybrides Unified Endpoint Management.

Während Intune eine effektive Verwaltung für überwiegend mobile Endgeräte bietet, erweitert ACMP diese Fähigkeiten auf die gesamte IT-Infrastruktur, einschließlich Clients, Server und weiteren IT-Komponenten. Die Integration von Intune in ACMP in einer einheitlichen Oberfläche erlaubt die zentrale Steuerung sämtlicher Endgeräte.

Unternehmen realisieren damit eine hybride UEM-Strategie sowohl über die Cloud (Intune) als auch die stationäre Infrastruktur (ACMP). In punkto Sicherheit, Effizienz oder Flexibilität müssen sie keine Kompromisse mehr eingehen. Durch die vereinfachte Verwaltung, automatisierte Prozesse und ein hohes Sicherheitsniveau bei der Endgeräteverwaltung leistet ein hybrides UEM einen wichtigen Beitrag zu einer zukunftsorientierten Ausrichtung jeder IT-Infrastruktur.

Über Aagon



„Manage any device in a connected world!“ – Seit 30 Jahren steht Aagon für innovative Client-Management- und Automationslösungen und ist führend in der Verwaltung von Endgeräten sowie der Automatisierung von Standardaufgaben. Durch sorgfältige Entwicklung, über 20 Jahre Markterfahrung und die enge Zusammenarbeit mit unseren Kunden und Partnern sind unsere Produkte optimal auf ihre Anforderungen und Bedürfnisse zugeschnitten.

Individuelle Beratung und die beste Unterstützung von Kunden und Partnern bei der Installation und Ersteinrichtung gehören bei Aagon zum Standard. Ein tiefes Verständnis für die Anforderungen unserer Kunden sowie der kontinuierliche Austausch mit ihnen und unseren Partnern ermöglichen eine Softwareentwicklung auf Augenhöhe. Webinare-on-Demand, vielfältiges Informationsmaterial wie Whitepaper, Ratgeber und Factsheets sowie die beliebten Anwendertreffen an Standorten in ganz Deutschland sind nur einige Beispiele dafür, wie kundennah und praxisorientiert ACMP entwickelt wird.

Aagon GmbH

Lange Wende 33

59494 Soest

Tel.: 02921 789 200

E-Mail: info@aagon.com

Web: www.aagon.com



Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.